Claims

1. A system for allowing common control of at least two virtual private network devices comprising:

at least two virtual private network devices each adapted to establish one or more encrypted data streams over an open network between a group of clients and a respective local area network; and

an authentication server and database that are accessed by said virtual private network devices;

wherein said authentication server verifies client credentials for said local area network thereby allowing maintenance of only a single authentication server and database for both of said virtual private network devices.

2. The system of claim 1 wherein said database stores network access information for said local area network for use by said virtual private network devices.

3. The system of claim 2 wherein said network access information includes a group identification.

4. The system of claim 3 wherein said database stores user identifications, passwords and customer identifications.

5. The system of claim 2 wherein said network access information includes address filters.

6. The system of claim 2 wherein said network access information includes device address filters.

7. The system of claim 2 wherein said network access information includes compression types.

8. The system of claim 2 wherein said network access information includes time access constraints.

9. The system of claim 2 wherein said network access information includes encryption types.

10. The system of claim 2 wherein said database is a directory service.

11. The system of claim 10 wherein said directory service is accessible via LDAP.

12. The system of claim 2 wherein said database is remote from said authentication server.

13. The system of claim 12 wherein said database is accessed over an open network.

14. The system of claim 12 wherein said database is accessed over a local area network.

15. A system for sharing a virtual private network device comprising:

a virtual private network device capable of establishing one or more encrypted data streams over an open network between a group of clients and a first private local

area network, and between a second group of clients and a second private local area network; and

an authentication server and database that are shared by said first and second private local area networks;

wherein said authentication server verifies client credentials stored in said database to control access by respective clients to both of said networks through said virtual private network device;

16. The system of claim 15 wherein said database stores local area network access information for said first and second private local area networks for use by said virtual private network device.

17. The system of claim 16 wherein said network access information includes a group identification.

18. The system of claim 16 wherein said network access information includes address filters.

19. The system of claim 16 wherein said network access information includes device address filters.

20. The system of claim 16 wherein said network access information includes compression types.

21. The system of claim 16 wherein said network access information includes time access constraints.

22. The system of claim 16 wherein said network access information includes encryption types.

23. The system of claim 17 wherein said database server stores user identifications, passwords and customer identifications.

24. The system of claim 16 wherein said database server is a directory service.

25. The system of claim 24 wherein said directory service is accessible via LDAP.

26. The system of claim 16 wherein said database is remote from said authentication server.

27. The system of claim 26 wherein said remote location is accessed over an open network.

28. The system of claim 26 wherein said remote location is accessed over a local area network.

29. A method for allowing common control of at least two private networking devices comprising:

configuring at least two virtual private network devices to connect to at least one local area network and an open network;

configuring said virtual private network devices to authenticate clients through use of a common database; and

maintaining said common database with client credentials for access to said at least one local area network through said open network using said virtual private network devices.

30. The method of claim 29 further comprising maintaining said common database with access information for use by said virtual private network devices.

31. The method of claim 30 wherein said access information includes a group identification.

32. The method of claim 30 wherein said access information includes address filters.

33. The method of claim 30 wherein said access information includes device address filters.

34. The method of claim 30 wherein said access information includes compression types.

35. The method of claim 30 wherein said access information includes time access constraints.

36. The method of claim 30 wherein said access information includes encryption types.

37. The method of claim 31 wherein said database stores user identifications, passwords and customer identifications.

38. The method of claim 29 wherein said database server is a directory service.

39. The method of claim 38 wherein said directory service is accessible via LDAP.

40. A method for sharing private network devices among private local area networks comprising:

configuring at least one virtual private network device to connect to a first private area network, a second private local area network and an open network;

configuring said virtual private network device to authenticate clients through use of a common database; and

maintaining said common database with credentials for clients of said first and second private local area networks.

41. The method of claim 40 further comprising maintaining said common database with access information for use by said virtual private network device.

42. The method of claim 41 wherein said access information includes a group identification.

43. The method of claim 41 wherein said access information includes address filters.

44. The method of claim 41 wherein said access information includes device address filters.

45. The method of claim 41 wherein said access information includes compression types.

46. The method of claim 41 wherein said access information includes time access constraints.

47. The method of claim 41 wherein said access information includes encryption types.

48. The method of claim 42 wherein said database stores user identifications, passwords and customer identifications.

49. The method of claim 40 wherein said database is a directory service.

50. The system of claim 49 wherein said directory service is accessible via LDAP.

51. A method for sharing virtual private network devices by multiple private local area networks comprising the steps of:

maintaining at least one virtual private network device connected to a plurality of private local area networks and an open network wherein said virtual private network device is capable of establishing encrypted data streams over an open network with clients of said plurality of private local area networks; and

maintaining client credentials and LAN access information for access to said private local area networks using said virtual private network device in a centralized database server;

52. The method of claim 51 further comprising:

maintaining an authentication server configured to access said database server and return said LAN access information to said virtual private network device.

53. The method of claims 51 or 52 wherein said LAN access information includes a group identification.

54. The method of claims 51 or 52 wherein said LAN access information includes address filters.

55. The method of claims 51 or 52 wherein said LAN access information includes device address filters.

56. The method of claims 51 or 52 wherein said LAN access information includes compression types.

57. The method of claims 51 or 52 wherein said LAN access information includes time access constraints.

58. The method of claims 51 or 52 wherein said LAN access information includes encryption types.

59. The method of claims 51 or 52 wherein said client credentials includes user identifications and passwords and said database server stores said client credentials with company names.

60. The method of claim 59 wherein said database server is a directory service.

61. The system of claim 60 wherein said directory service is accessible via LDAP.